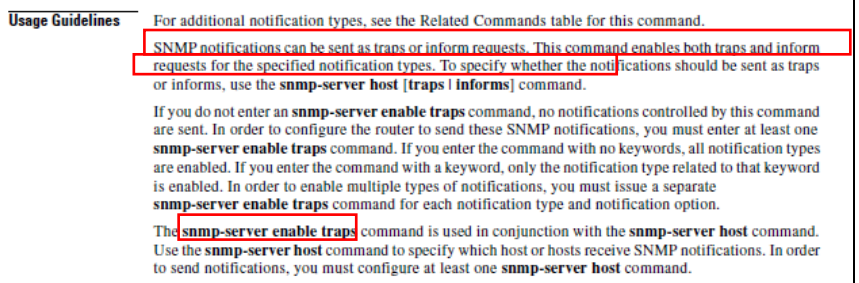
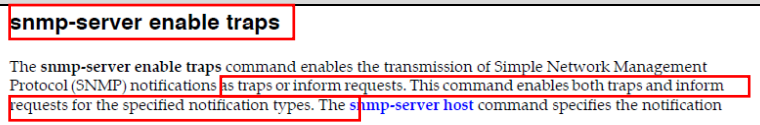
Ex. F

Exhibit Copying-1 – Evidence of Documentation Copying

Copyright Registration Information	Cisco	Arista
Cisco IOS XE 3.5 Effective date of registration: 11/24/2014	 **Usage Guidelines** For additional notification types, see the Related Commands table for this command. SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps**	**informs**] command. If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option. The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command. Cisco IOS Configuration Fundamentals and Network Management Command Reference (2004), at 1034; *see also* Cisco IOS Asynchronous Transfer Mode Command Reference (2011), at 535.	 **snmp-server enable traps** The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The **snmp-server host** command specifies the notification Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1990. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 (11/18/11), at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.

Copyright Registration Information	Cisco	Arista
Cisco IOS XE 3.5 Effective date of registration: 11/24/2014	Router# **show interfaces atm 0/0/0** ATM0/0/0 is up, line protocol is up Hardware is cyBus ATM Internet address is 10.1.1.1/24 MTU 4470 bytes, sub MTU 4470, BW 156250 Kbit, DLY 80 usec, rely 255/255, load 1/255 Encapsulation ATM, loopback not set, keepalive set (10 sec) Encapsulation(s): AAL5, PVC mode 256 TX buffers, 256 RX buffers, 2048 maximum active VCs, 1024 VCs per VP, 1 current VCCs VC idle disconnect time: 300 seconds Last input never, output 00:00:05, output hang never Last clearing of "show interface" counters never Queueing strategy: fifo Output queue 0/40, 0 drops; input queue 0/75, 0 drops 5 minute input rate 0 bits/sec, 1 packets/sec 5 minute output rate 0 bits/sec, 1 packets/sec 5 packets input, 560 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 5 packets output, 560 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets 0 output buffer failures, 0 output buffers swapped out Cisco IOS Asynchronous Transfer Mode Command Reference (2011), at 476.	Examples • These commands display interface counters, clear the counters, then display the counters again. switch#**show interfaces ethernet 1** Ethernet1 is up, line protocol is up (connected) Hardware is Ethernet, address is 001c.7302.2fff (bia 001c.7302.2fff) MTU 9212 bytes, BW 10000000 Kbit Full-duplex, 10Gb/s, auto negotiation: off Last clearing of "show interface" counters never 5 minutes input rate 101 bps (0.0% with framing), 0 packets/sec 5 minutes output rate 0 bps (0.0% with framing), 0 packets/sec 228537085400 packets input, 225028582832583 bytes Received 29769609741 broadcasts, 3073437605 multicast 113 runts, 1 giants 118 input errors, 117 CRC, 0 alignment, 18 symbol 27511409 PAUSE input 335031607678 packets output, 27845413138330 bytes Sent 14282316688 broadcasts, 54045824072 multicast 108 output errors, 0 collisions 0 late collision, 0 deferred 0 PAUSE output Arista User Manual v. 4.13.6F (4/14/2014), at 637. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 514; Arista User Manual, v. 4.11.1 (1/11/13), at 413; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.
Cisco IOS XE 3.5 Effective date of registration: 11/24/2014	**show vrrp** To display a brief or detailed status of one or all configured Virtual Router Redundancy Protocol (VRRP) groups on the router, use the **show vrrp** command in privileged EXEC mode. **show vrrp [all | brief]** Cisco IOS IP Application Services Command Reference (2011), at 76.	19.2.3.2 Verify VRRP IPv6 Configurations Use the following commands to display the VRRP configurations and status. **Show VRRP Group** The show vrrp command displays the status of configured Virtual Router Redundancy Protocol (VRRP) groups on a specified interface. Arista User Manual v. 4.13.6F (4/14/2014), at 879. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 793; Arista User Manual v. 4.10.3 (10/22/12), at 548; Arista User Manual v. 4.9.3.2 (5/3/12), at 468.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Usage Guidelines** Use the **ip multicast multipath** command to enable load splitting of IP multicast traffic across multiple equal-cost paths. If two or more equal-cost paths from a source are available, unicast traffic will be load split across those paths. However, by default, multicast traffic is not load split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the Protocol Independent Multicast (PIM) specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric. Configuring load splitting with the **ip multicast multipath** command causes the system to load split multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the **ip multicast multipath** command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups. Cisco IOS IP Multicast Command Reference (2011), at 293.	23.3.2 Equal Cost Multipath Routing (ECMP) and Load Sharing Multiple routes that have identical destinations and administrative distances comprise an Equal Cost Multi-Path (ECMP) route. The switch attempts to spread traffic to all ECMP route paths equally. If two or more equal-cost paths from a source are available, unicast traffic is load split across those paths. By default, multicast traffic is not load split. Multicast traffic generally flows from the reverse path forwarding (RPF) neighbor and, according to Protocol Independent Multicast (PIM) specifications, the neighbor with the highest IP address has precedence when multiple neighbors have the same metric. Arista User Manual v. 4.13.6F (4/14/2014), at 1191. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1042; Arista User Manual, v. 4.11.1 (1/11/13), at 398; Arista User Manual v. 4.10.3 (10/22/12), at 320.
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Usage Guidelines** Use the **ip multicast boundary** command to configure an administratively scoped boundary on an interface in order to filter source traffic coming into the interface and prevent mroute states from being created on the interface. **Note** An IP multicast boundary enables reuse of the same multicast group address in different administrative domains. Cisco IOS IP Multicast Command Reference (2011), at 264.	**Multicast Boundary Configuration** The multicast boundary specifies subnets where source traffic entering an interface is filtered to prevent the creation of mroute states on the interface. The interface is not included in the outgoing interface list (OIL). Multicast pim, igmp or data packets are not allowed to flow across the boundary from either direction. The boundary facilitates the use of a multicast group address in different administrative domains. The **ip multicast boundary** command configures the multicast boundary. The multicast boundary can be specified through multiple IPv4 subnets or one standard IPv4 ACL. Arista User Manual v. 4.13.6F (4/14/2014), at 1704. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1482; Arista User Manual, v. 4.11.1 (1/11/13), at 1184; Arista User Manual v. 4.10.3 (10/22/12), at 1018; Arista User Manual v. 4.9.3.2 (5/3/12), at 776.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.0 Effective Date of Registration: 11/28/2014	**Usage Guidelines** Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface. An interface can be configured to be in dense mode, sparse mode, or sparse-dense mode. The mode describes how the Cisco IOS software populates its multicast routing table and how the software forwards multicast packets it receives from its directly connected LANs. Dense mode interfaces are always added to the table when the multicast routing table is populated. Sparse mode interfaces are added to the table only when periodic join messages are received from downstream routers, or there is a directly connected member on the interface. Cisco IOS IP Multicast Command Reference (2008), at IMC-233–34	33.3.1 Enabling IGMP Enabling PIM on an interface also enables IGMP on that interface. When the switch populates the multicast routing table, interfaces are added to the table only when periodic join messages are received from downstream routers, or when there is a directly connected member on the interface. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1778. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1726; Arista User Manual v. 4.12.3 (7/17/13), at 1504; Arista User Manual, v. 4.11.1 (1/11/13), at 1204; Arista User Manual v. 4.10.3 (10/22/12), at 998; Arista User Manual v. 4.9.3.2 (5/3/12), at 756; Arista User Manual v. 4.8.2 at 578; Arista User Manual v. 4.7.3 (7/18/11), at 458; Arista User Manual v. 4.6.0 (12/22/2010), at 308
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Usage Guidelines** SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml . Cisco IOS IP Multicast Command Reference (2011), at 742	SNMP Commands Chapter 37 SNMP **snmp-server enable traps** The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The **snmp-server host** command specifies the notification type (traps or informs). Sending notifications requires at least one **snmp-server host** command. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1990. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Usage Guidelines** The local proxy ARP feature allows the Multilayer Switching Feature Card (MSFC) to respond to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, the MSFC responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the Catalyst 6500 series switch on which they are connected. Before the local proxy ARP feature can be used, the IP proxy ARP feature must be enabled. The IP proxy ARP feature is enabled by default. Cisco IOS IP Addressing Services Command Reference (2011), at 394	**ip local-proxy-arp** The **ip local-proxy-arp** command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1276. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 856; Arista User Manual v. 4.10.3 (10/22/12), at 707.
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Usage Guidelines** IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 10.108.11.0 255.255.255.0. Cisco IOS IP Addressing Services Command Reference (2011), at 452	• ***SUBNET_SIZE*** this functions as a sanity check to ensure it is not a network or broadcast network. Options include: — **netmask** *ipv4_addr* The network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong (dotted decimal notation). Arista User Manual v. 4.13.6F (4/14/2014), at 1233. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1075.

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. **IP Extended Community-List Configuration Mode** Named and numbered extended community lists can be configured in IP Extended community-list configuration mode. To enter IP Extended community-list configuration mode, enter the **ip extcommunity-list** command with either the **expanded** or **standard** keyword followed by the extended community list name. This configuration mode supports all of the functions that are available in global configuration mode. In addition, you can perform the following operations: Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IRP-118	**ip extcommunity-list expanded** The **ip extcommunity-list expanded** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list. • **Route Target (rt)** attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • **Site of Origin (soo)** attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 at 519.
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Usage Guidelines** Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). The **match extcommunity** command is used to configure match clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes. Cisco IOS IP Routing: EIGRP Command Reference (2011), at 92	BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Extended community clauses provide route target and site of origin parameter options: Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11) at 500.

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**Expanded Community Lists** Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the Regular Expressions appendix of the *Cisco IOS Terminal Services Configuration Guide*. Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IRP-113–14	**Chapter 3 Command-Line Interface** **Processing Commands** ^rxy$ ^rxy 23 21 rxy ,rxy, rxy ,rxy. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 107. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	Router# **show ip route** Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route Gateway of last resort is not set Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IP2R-553	**IPv4 Routing** **Chapter 23 IPv4** **Examples** • This command displays IP routes learned through BGP. switch>**show ip route bgp** Codes: C - connected, S - static, K - kernel, O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type2, B I - iBGP, B E - eBGP, R - RIP, A - Aggregate B E 170.44.48.0/23 [20/0] via 170.44.254.78 B E 170.44.50.0/23 [20/0] via 170.44.254.78 B E 170.44.52.0/23 [20/0] via 170.44.254.78 B E 170.44.54.0/23 [20/0] via 170.44.254.78 B E 170.44.254.112/30 [20/0] via 170.44.254.78 B E 170.53.0.34/32 [1/0] via 170.44.254.78 B I 170.53.0.35/32 [1/0] via 170.44.254.2 via 170.44.254.13 via 170.44.254.20 via 170.44.254.67 via 170.44.254.35 via 170.44.254.98 switch> Arista User Manual v. 4.13.6F (4/14/2014), at 1188. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1039; Arista User Manual, v. 4.11.1 (1/11/13), at 838; Arista User Manual v. 4.10.3 (10/22/12), at 685.

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**Usage Guidelines** The **clear ip bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions. Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IRP-69	**clear ip bgp** The **clear ip bgp** command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required. • a hard reset tears down and rebuilds the peering sessions and rebuilds BGP routing tables. • a soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft resets use stored update information to apply new BGP policy without disrupting the network. Routes that are read or sent are processed through modified route maps or AS-path access lists. The command can also clear the switch's BGP sessions with its peers. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014, at 1577. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1527; Arista User Manual v. 4.12.3 (7/17/13), at 1358; Arista User Manual, v. 4.11.1 (1/11/13), at1104; Arista User Manual v. 4.10.3 (10/22/12), at 916; Arista User Manual v. 4.9.3.2 (5/3/12), at 683; Arista User Manual v. 4.8.2 (11/18/11), at 513; Arista User Manual v. 4.7.3 (7/18/11), at 378.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**max-metric router-lsa** To configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric router-lsa** command in router configuration mode. To disable the advertisement of a maximum metric, use the **no** form of this command. **max-metric router-lsa [on-startup** {*seconds* | **wait-for-bgp**}**]** **no max-metric router-lsa [on-startup** {*seconds* | **wait-for-bgp**}**]** Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IP2R-591	Chapter 25 Open Shortest Path First – Version 2 OSPFv2 Commands **max-metric router-lsa (OSPFv2)** The **max-metric router-lsa** command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations. The **no max-metric router-lsa** and **default max-metric router-lsa** commands disable the advertisement of a maximum metric. **Platform** all **Command Mode** Router-OSPF Configuration **Command Syntax** `max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]` `no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]` `default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]` All parameters can be placed in any order. Arista User Manual v. 4.13.6F (4/14/2014), at 1389.

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**adv-router** [*ip-address*] — (Optional) Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as **self-originate**). *link-state-id* — (Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address. When the link state advertisement is describing a network, the *link-state-id* can take one of two forms: The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements). A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IP2R-613	• *linkstate_id* Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. — When the LSA describes a network, the *linkstate-id* argument is one of the following: The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1454. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 648; Arista User Manual v. 4.8.2 (11/18/11), at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217.

Copyright Registration Information	Cisco	Arista
Cisco XE 3.5 Effective date of registration: 11/24/2014	**area nssa translate** To configure a not-so-stubby area (NSSA) and to configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, use the **area nssa translate**command in router address family topology or router configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command. **area nssa translate commandarea** *area-id* **nssa translate type7 [always] [suppress-fa] [default-information-originate [metric** *ospf-metric*] **[metric-type** *ospf-link-state-type*] **[nssa-only]] [no-ext-capability] [no-redistribution] [no-summary]** **no area** *area-id* **nssa translate type7 [always] [suppress-fa] [default-information-originate [metric** *ospf-metric*] **[metric-type** *ospf-link-state-type*] **[nssa-only]] [no-ext-capability] [no-redistribution] [no-summary]** **Syntax Description** *area-id* — Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address. **translate** — Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR). **type7** — (Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR. **always** — (Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the **always** keyword only in router configuration mode, not in router address family topology configuration mode. Cisco IOS IP Routing: OSPF Command Reference (2011), at 15	Chapter 26 Open Shortest Path First – Version 3 OSPFv3 Commands **area nssa translate type7 always (OSPFv3)** The **area nssa translate type7 always** command translates Type-7 link-state advertisement (LSA) to Type-5 of LSAs. The **no area nssa translate type7 always** command removes the NSSA distinction from the area. Platform all Command Mode Router-OSPF3 Configuration Command Syntax `area area_id nssa translate type7 always` `no area_id nssa translate type7 always` `default area_id nssa translate type7 always` Parameters • *area_id* area number. Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255> Area 0 (or 0.0.0.0) is not configurable; it is always *normal*. ***Running-config*** stores value in dotted decimal notation. Example • This command configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. `switch(config)#ipv6 router ospf 3` `switch(config-router-ospf3)#area 3 nssa translate type7 always` `switch(config-router-ospf)#` Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1501. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1451; Arista User Manual v. 4.12.3 (7/17/13), at 1286; Arista User Manual, v. 4.11.1 (1/11/13), at 1036.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 12.4

Effective date of registration: 8/12/2005</td>
<td>
timers basic (RIP)

To adjust Routing Information Protocol (RIP) network timers, use the timers basic command in router configuration mode. To restore the default timers, use the no form of this command.

timers basic update invalid holddown flush

no timers basic

<table>
<tr><td>Syntax Description</td><td>update</td><td>Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.</td></tr>
<tr><td></td><td>invalid</td><td>Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the update argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a holddown state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 90 seconds.</td></tr>
<tr><td></td><td>holddown</td><td>Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the update argument. A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 180 seconds.</td></tr>
<tr><td></td><td>flush</td><td>Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified should be greater than the value of the invalid argument. If it is less than this sum, the proper holddown interval cannot elapse, which results in a new route being accepted before the holddown interval expires. The default is 240 seconds.</td></tr>
</table>

Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IRP-811
</td>
<td>
Chapter 28 Routing Information Protocol RIP Commands

timers basic (RIP)

The timers basic command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values.
• The update time is the interval between unsolicited route responses. The default is 30 seconds.
• The expiration time is initialized when a route is established and any time an update is received for the route. If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds.
• The deletion time is initialized when the expiration time has elapsed. On initialization of the deletion time, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped. Upon expiration of the deletion time, the route is removed from the routing table. The default is 120 seconds.

Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1671,

See also Arista User Manual v. 4.13.6F (4/14/2014), at 1621; Arista User Manual v. 4.12.3 (7/17/13), at 1433; Arista User Manual, v. 4.11.1 (1/11/13), at 1179; Arista User Manual v. 4.10.3 (10/22/12), at 989; Arista User Manual v. 4.9.3.2 (5/3/12), at 748; Arista User Manual v. 4.8.2 at 570.
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination. Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network. If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host. To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host. Cisco IOS IP Switching Command Reference (2011), v. 15.2, at 542	37.2.2 SNMP Notifications SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A *trap* is an unsolicited notification. An *inform* (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses. Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead. Table 37-2 lists the SNMP traps that the switch supports. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination. Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network. Cisco IOS Network Management Command Reference (2005), at 522	37.2.2 SNMP Notifications SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A *trap* is an unsolicited notification. An *inform* (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses. Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead. Table 37-2 lists the SNMP traps that the switch supports. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.

Copyright Registration Information	Cisco	Arista
Cisco IOS XE 3.5 Effective date of registration: 11/24/2014	Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network. Cisco IOS IP Switching Command Reference (2011), v. XE 3.5, at 544.	SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A *trap* is an unsolicited notification. An *inform* (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses. Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.
Cisco IOS XE 2.1 Effective date of registration: 11/24/2014	Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network. Cisco IOS IP Switching Command Reference (2008), at ISW-344.	SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A *trap* is an unsolicited notification. An *inform* (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses. Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	*Table 22 show ip bgp neighbors paths Field Descriptions* **Field** / **Description** Address — Internal address where the path is stored. Refcount — Number of routes using that path. **Field** / **Description** Metric — Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.) Path — Autonomous system path for that route, followed by the origin code for that route. Cisco IOS Multiprotocol Label Switching Command Reference (2011), at 640-41.	**show ip bgp paths** The **show ip bgp paths** command displays all BGP paths in the database. **Platform** all **Command Mode** EXEC **Command Syntax** `show ip bgp paths [VRF_INSTANCE]` **Parameters** • *VRF_INSTANCE* specifies VRF instances. — <no parameter> displays routing table for context-active VRF. — **vrf** *vrf_name* displays routing table for the specified VRF. — **vrf all** displays routing table for all VRFs. — **vrf default** displays routing table for default VRF. **Display Values** • **Refcount**: Number of routes using a listed path. • **Metric**: The Multi Exit Discriminator (MED) metric for the path. • **Path**: The autonomous system path for that route, followed by the origin code for that route. The MED, also known as the external metric of a route, provides information to external neighbors about the preferred path into an AS with multiple entry points. Lower MED values are preferred. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 776; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249.

Copyright Registration Information	Cisco	Arista
Cisco IOS XE 2.1 Effective date of registration: 11/24/2014	*Table 28 show ip bgp neighbors paths Field Descriptions* **Field** / **Description** Address — Internal address where the path is stored. Refcount — Number of routes using that path. Metric — Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.) Path — Autonomous system path for that route, followed by the origin code for that route. Cisco IOS Multiprotocol Label Switching Command Reference (2008), at 475.	**show ip bgp paths** The **show ip bgp paths** command displays all BGP paths in the database. Platform all Command Mode EXEC Command Syntax `show ip bgp paths [VRF_INSTANCE]` Parameters • *VRF_INSTANCE* specifies VRF instances. — <no parameter> displays routing table for context-active VRF. — **vrf** *vrf_name* displays routing table for the specified VRF. — **vrf all** displays routing table for all VRFs. — **vrf default** displays routing table for default VRF. Display Values • **Refcount**: Number of routes using a listed path. • **Metric**: The Multi Exit Discriminator (MED) metric for the path. • **Path**: The autonomous system path for that route, followed by the origin code for that route. The MED, also known as the external metric of a route, provides information to external neighbors about the preferred path into an AS with multiple entry points. Lower MED values are preferred. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 776; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Usage Guidelines** This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process. In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication. Cisco IOS HTTP Services Configuration Guide (2011), at 49.	**protocol https certificate (API Management)** The **protocol https certificate** command configures the HTTP secure server to request an X.509 certificate from the client to configure the server certificate. The client (usually a web browser), in turn, has a public key that allows it to authenticate the certificate. The **no protocol https certificate** and **default protocol https certificate** commands restore default behavior by removing the **protocol https certificate** statement from *running-config*. **Platform** all **Command Mode** Mgmt-api Configuration **Command Syntax** `protocol https certificate` `no protocol https certificate` `default protocol https certificate` **Related Commands** • management api http-commands places the switch in Management-api configuration mode. **Examples** • These commands configures the HTTP server to request an X.509 certificate from the client in order to authenticate the client during the connection process. `switch(config)#management api http-commands` `switch(config-mgmt-api-http-cmds)#protocol https certificate` `switch(config-mgmt-api-http-cmds)#` Arista User Manual v. 4.13.6F (4/14/2014), at 85. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 75.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Usage Guidelines** To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** command with the **remote** keyword. The remote agent's Cisco IOS SNMP Support Command Reference (2011), at 380	**Configuring the Group** An SNMP group is a table that maps SNMP users to SNMP views. The **snmp-server group** command configures a new SNMP group. **Example** • This command configures *normal_one* as an SNMPv3 group (authentication and encryption) that provides access to the *all-items* read view. `switch(config)#snmp-server group normal_one v3 priv read all-items` `switch(config)#` **Configuring the User** An SNMP user is a member of an SNMP group. The **snmp-server user** command adds a new user to an SNMP group and configures that user's parameters. To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1894; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1344; Arista User Manual v. 4.10.3 (10/22/12), at 1110; Arista User Manual v. 4.9.3.2 (5/3/12), at 865; Arista User Manual v. 4.8.2 (11/18/11), at 677; Arista User Manual v. 4.7.3 (7/18/11), at 533.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.2

Effective date of registration:

11/24/2014</td>
<td>
Usage Guidelines The show snmp host command displays details such as IP address of the Network Management System (NMS), notification type, SNMP version, and the port number of the NMS.
To configure these details, use the snmp-server hostcommand.

Command Examples The following is sample output from the show snmp hostcommand.

<pre>Router# show snmp host
Notification host: 10.2.28.6 udp-port: 162   type: inform
user: public   security model: v2c
traps: 00001000.00000000.00000000</pre>
The table below describes the significant fields shown in the display.

Table 5 show snmp host Field Descriptions
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Notification host</td><td>Displays the IP address of the host for which the notification is generated.</td></tr>
<tr><td>udp-port</td><td>Displays the port number.</td></tr>
<tr><td>type</td><td>Displays the type of notification.</td></tr>
<tr><td>user</td><td>Displays the access type of the user for which the notification is generated.</td></tr>
<tr><td>security model</td><td>Displays the SNMP version used to send notifications.</td></tr>
<tr><td>traps</td><td>Displays details of the notification generated.</td></tr>
</table>

Cisco IOS SNMP Support Command Reference (July 2011), at 108–09
</td>
<td>
SNMP Commands Chapter 37 SNMP

show snmp host

The show snmp host command displays the recipient details for Simple Network Management Protocol (SNMP) notification operations. Details that the command displays include IP address and port number of the Network Management System (NMS), notification type, and SNMP version.

Platform all
Command Mode EXEC

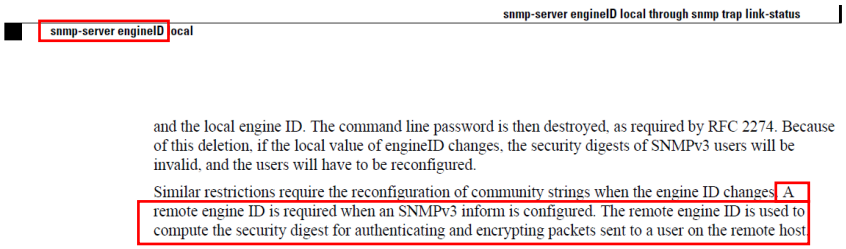
Command Syntax
show snmp host

Field Descriptions
• Notification host IP address of the host for which the notification is generated.
• udp-port port number.
• type notification type.
• user access type of the user for which the notification is generated.
• security model SNMP version used to send notifications.
• traps details of the notification generated.

Arista User Manual v. 4.13.6F (4/14/2014), at 1908

See also Arista User Manual v.4.14.3F (Rev. 2) (10/2/2014), at 1980; Arista User Manual v. 4.12.3 (7/17/13), at 1670; Arista User Manual, v. 4.11.1 (1/11/13), at 1357; Arista User Manual v. 4.10.3 (10/22/12), at 1124; Arista User Manual v. 4.9.3.2 (5/3/12), at 880; Arista User Manual v. 4.8.2 (11/18/11), at 688; Arista User Manual v. 4.7.3 (7/18/11), at 544.
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**show snmp view** To display the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and associated MIB, use the **show snmp view**command in privileged EXEC mode. Cisco IOS SNMP Support Command Reference (2011), at 140	SNMP Commands Chapter 37 SNMP **show snmp view** The **show snmp view** command displays the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and the associated MIB. SNMP views are configured with the **snmp-server view** command. **Platform** all **Command Mode** EXEC Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1986. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1914; Arista User Manual v. 4.12.3 (7/17/13), at 1676; Arista User Manual, v. 4.11.1 (1/11/13), at 1361; Arista User Manual v. 4.10.3 (10/22/12), at 1128; Arista User Manual v. 4.9.3.2 (5/3/12), at 884; Arista User Manual v. 4.8.2 (11/18/11), at 692; Arista User Manual v. 4.7.3 (7/18/11), at 548.
Cisco IOS 15.2 Effective date of registration: 11/24/20141	**Usage Guidelines** This command provides counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** global configuration command. **Command Examples** The following is sample output from the **show snmp** command: Router# **show snmp** Chassis: 12161083 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 Input queue packet drops (Maximum queue size 1000) 0 SNMP packets output 0 Too big errors (Maximum packet size 1500) 0 No such name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs SNMP logging: enabled Cisco IOS SNMP Support Command Reference (2011), at 95-96	Configuring SNMP Chapter 37 SNMP 8 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 8 Number of requested variables 0 Number of altered variables 4 Get-request PDUs 4 Get-next PDUs 0 Set-request PDUs 21 SNMP packets output 0 Too big errors 0 No such name errors 0 Bad value errors 0 General errors 8 Response PDUs 0 Trap PDUs SNMP logging: enabled Logging to taccon.162 SNMP agent enabled switch(config)# Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1967-68. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1896; Arista User Manual v. 4.12.3 (7/17/13), at 1658; Arista User Manual, v. 4.11.1 (1/11/13), at 1345; Arista User Manual v. 4.10.3 (10/22/12), at 1091; Arista User Manual v. 4.9.3.2 (5/3/12), at 868; Arista User Manual v. 4.8.2 (11/18/11), at 678; Arista User Manual v. 4.7.3 (7/18/11), at 534.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	 Cisco IOS SNMP Support Command Reference (2011), at 324.	**snmp-server engineID remote** The **snmp-server engineID remote** command configures the name of a Simple Network Management Protocol (SNMP) engine located on a remote device. The switch generates a default engineID; use the **show snmp engineID** command to view the configured or default engineID. A remote engine ID is required when configuring an SNMPv3 inform to compute the security digest for authenticating and encrypting packets sent to users on the remote host. SNMPv3 authenticates users through security digests (MD5 or SHA) that are based on user passwords and the engine ID. Passwords entered on the CLI are similarly converted, then compared to the user's security digest to authenticate the user. Arista User Manual v. 4.13.6F (4/14/2014), at 1920. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1682; Arista User Manual, v. 4.11.1 (1/11/13), at 1367; Arista User Manual v. 4.10.3 (10/22/12), at 1134; Arista User Manual v. 4.9.3.2 (5/3/12), at 890; Arista User Manual v. 4.8.2 (11/18/11), at 698; Arista User Manual v. 4.7.3 (7/18/11), at 554.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**aaa group server radius** To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command. **aaa group server radius** *group-name* **no aaa group server radius** *group-name* Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-74.	**aaa group server radius** The **aaa group server radius** command enters the server-group-radius configuration mode for the specified group name. The command creates the specified group if it was not previously created. Commands are available to add servers to the group. A server group is a collection of servers that are associated with a single label. Subsequent authorization and authentication commands access all servers in a group by invoking the group name. Server group members must be previously configured with a **radius-server host** command. The **no aaa group server radius** and **default aaa group server radius** commands delete the specified server group from *running-config*. **Platform** all **Command Mode** Global Configuration **Command Syntax** `aaa group server radius group_name` `no aaa group server radius group_name` `default aaa group server radius group_name` Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 224. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 217; Arista User Manual v. 4.12.3 (7/17/13), at 168; Arista User Manual, v. 4.11.1 (1/11/13), at 126; Arista User Manual v. 4.10.3 (10/22/12), at 118.

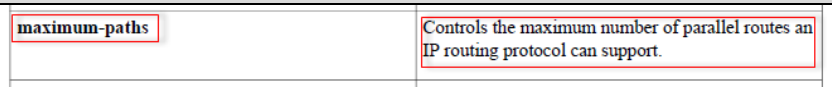
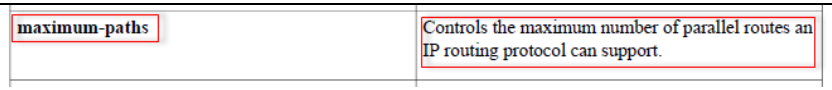
Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**aaa authentication dot1x** To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-32.	11.3.1 Configuring an Authentication Method List for 802.1x To use 802.1x port security, specify an authentication method to be used to authenticate clients. The switch supports RADIUS authentication with 802.1x port security. To use RADIUS authentication with 802.1x port security, you create an authentication method list for 802.1x and specify RADIUS as an authentication method, then configure communication between the switch and RADIUS server. Example • The aaa authentication dot1x command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. The following example uses the aaa authentication dot1x command with RADIUS authentication. `switch> enable` `switch# configure terminal` `switch(config)# aaa authentication dot1x default group radius` Arista User Manual v. 4.13.6F (4/14/2014), at 551,
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**dot1x port-control** To set an 802.1X port control value, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command. **dot1x port-control {auto | force-authorized | force-unauthorized}** **no dot1x port-control {auto | force-authorized | force-unauthorized}** Syntax Description **auto** — Determines authentication status of the client PC by the authentication process. The port state will be set to AUTO. **force-authorized** — Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default. **force-unauthorized** — Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-457.	Example • This command configures Ethernet 1 to immediately commence functioning as authenticator ports. `switch(config)#interface ethernet 1` `switch(config-if-Et1)#dot1x port-control auto` `switch(config-if-Et1)#` The dot1x port-control force-authorized command causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. Example • This example of the command designates Ethernet 1 as an authenticator port that is to continue to forward packets. `switch(config)#interface ethernet 1` `switch(config-if-Et1)#dot1x port-control force-authorized` `switch(config-if-Et1)#` Example • The dot1x port-control force-unauthorized command places the specified ports in the state of unauthorized, denying any access requests from users of the ports. `switch(config)#interface ethernet 1` `switch(config-if-Et1)#dot1x port-control force-authorized` `switch(config-if-Et1)#` Arista User Manual v. 4.13.6F (4/14/2014), at 552,

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**dot1x max-reauth-req** To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client, use the **dot1x max-reauth-req**command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the **no** form of this command. **dot1x max-reauth-req** *number* **no dot1x max-reauth-req** Cisco IOS Security Command Reference: Commands D to L (2011), at 164.	11.3.5 Setting the Maximum Number of Times the Authenticator Sends EAP Request The **dot1x max-reauth-req** command sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state. Example • These commands set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame to the client. `switch(config)#interface ethernet 1` `switch(config-if-Et1)#dot1x max-reauth-req 4` `switch(config-if-Et1)#` Arista User Manual v. 4.13.6F (4/14/2014), at 553,
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**dot1x pae** To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command. **dot1x pae [supplicant | authenticator | both]** **no dot1x pae [supplicant | authenticator | both]** **Syntax Description** **supplicant** — (Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator. **authenticator** — (Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant. **both** — (Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages. Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-456.	**dot1x pae authenticator** The **dot1x pae authenticator** command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant. The **no dot1x pae authenticator** and **default dot1x pae authenticator** commands restore the switch default by deleting the corresponding **dot1x pae authenticator** command from *running-config*. **Platform** all **Command Mode** Interface-Ethernet Configuration Interface-Management Configuration Arista User Manual v. 4.13.6F (4/14/2014), at 560.

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**dot1x timeout (EtherSwitch)** To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the **dot1x timeout** command in global configuration mode. To return to the default setting, use the **no** form of this command. **dot1x timeout** {**quiet-period** *seconds* | **re-authperiod** *seconds* | **tx-period** *seconds*} **no dot1x timeout** {**quiet-period** *seconds* | **re-authperiod** *seconds* | **tx-period** *seconds*} **Syntax Description** **quiet-period** *seconds* Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds. Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-466.	**dot1x timeout quiet-period** The **dot1x timeout quiet-period** command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.The range is 1 to 65535 seconds; the default is 60. When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default. The **no dot1x timeout quiet-period** and **default dot1x timeout quiet-period** commands restore the default advertisement interval of 60 seconds by removing the corresponding **dot1x timeout quiet-period** command from *running-config*. **Platform** all **Command Mode** Interface-Ethernet Configuration Interface-Management Configuration Arista User Manual v. 4.13.6F (4/14/2014), at 563,
Cisco IOS 12.4 Effective date of registration: 8/12/2005	**Usage Guidelines** The **security passwords min-length** command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as "lab" and "cisco." This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail. Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-943.	**password minimum length (Security Management)** The **password minimum length** command provides enhanced security access to the switch by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks. This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail. Applicable CC Requirements: The switch settings for secure passwords can be found under secure preparation. The password minimum length should be 15 characters and SHA-512 should be used as the hashing mechanism for all locally stored passwords. Arista User Manual v. 4.13.6F (4/14/2014), at 152,

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.2 Effective date of registration: 11/24/2014	**Command Examples** This example shows the output from the **show port-security** command when you do not enter any options: `Router# show port-security` `Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action` `(Count) (Count) (Count)` `Fa5/1 11 11 0 Shutdown` `Fa5/5 15 5 0 Restrict` `Fa5/11 5 4 0 Protect` `Total Addresses in System: 21` `Max Addresses limit in System: 128` `Router#` Cisco IOS Security Command Reference Commands S to Z (July 2011), at 692.	**Example** • These commands enable MAC security on Ethernet interface 7, set the maximum number of assigned MAC addresses to 2, assigns two static MAC addresses to the interface, and clears the dynamic MAC addresses for the interface. `switch(config)#interface ethernet 7` `switch(config-if-Et7)#switchport port-security` `switch(config-if-Et7)#switchport port-security maximum 2` `switch(config-if-Et7)#exit` `switch(config)#mac address-table static 0034.24c2.8f11 vlan 10 interface ethernet 7` `switch(config)#mac address-table static 4464.842d.17ce vlan 10 interface ethernet 7` `switch(config)#clear mac address-table dynamic interface ethernet 7` `switch(config)#show port-security` `Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action` `(Count) (Count) (Count)` `Et7 2 2 0 Shutdown` Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 632. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405-06; Arista User Manual v. 4.10.3 (10/22/12), at 336.

Copyright Registration Information	Cisco	Arista
Cisco IOS XE 3.5 Effective date of registration: 11/24/2014	**Command Modes** PTP clock configuration (config-ptp-clk) **Command History** **Release** — **Modification** 15.0(1)S — This command was introduced. **Usage Guidelines** Slave devices use the priority1 value when selecting a master clock. The priority1 value has precedence over the priority2 value. Cisco IOS Interface and Hardware Component Command Reference (2011), at 1018.	**ptp priority1** The **ptp priority1** command configures the priority1 value to use when advertising the clock. This value overrides the default criteria for best master clock selection. Lower values take precedence. The range is from 0 to 255. To remove PTP settings, use the **no** form of this command. **Platform** FM6000 **Command Mode** Global Configuration **Command Syntax** `ptp priority1 priority_rate` `no ptp priority1` `default ptp priority1` **Parameters** • *priority_rate* The value to override the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. Value ranges from 0 to 255. The default is 128. **Examples** • This command configures the preference level for a clock: slave devices use the priority1 value when selecting a master clock. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Cisco IOS IP Routing: BGP Command Reference (2013), at 375.	**maximum-paths (OSPFv2)** The **maximum-paths** command controls the maximum number of parallel routes that OSPFv2 supports on the switch. The default maximum is 16 paths. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1440. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1226; Arista User Manual, v. 4.11.1 (1/11/13), at 983; Arista User Manual v. 4.10.3 (10/22/12), at 813; Arista User Manual v. 4.9.3.2 (5/3/12), at 637; Arista User Manual v. 4.8.2 (11/18/11), at 472.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 146.	**maximum-paths (OSPFv2)** The **maximum-paths** command controls the maximum number of parallel routes that OSPFv2 supports on the switch. The default maximum is 16 paths. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1440. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1226; Arista User Manual, v. 4.11.1 (1/11/13), at 983; Arista User Manual v. 4.10.3 (10/22/12), at 813; Arista User Manual v. 4.9.3.2 (5/3/12), at 637; Arista User Manual v. 4.8.2 (11/18/11), at 472.